IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. MARK E. TOLSON, *Defendant.*	Case No. 1:19-CR-269 The Honorable Leonie M. Brinkema Sentencing date: December 20, 2019

POSITION OF THE UNITED STATES WITH RESPECT TO SENTENCING

Defendant Mark E. Tolson's decision to unlawfully access another person's email account on October 30 and 31, 2018, was not a momentary lapse in judgment. Over the course of two days, the defendant plotted how he would break into another person's email account and then carried out the crime. To be sure, the defendant's primary motivation was to protect a federal official and that official's investigation from what he perceived to be scurrilous accusations of misconduct. Yet, as an employee of the Federal Bureau of Investigation, the defendant knew better than to take the law into his own hands. He understood that vigilantism—no matter the cause being pursued—undermines justice.

The United States acknowledges that the defendant has accepted responsibility and entered an early plea that has saved government resources. Nonetheless, in light of the seriousness of the defendant's conduct, the need to promote respect for the law, and the need for deterrence, the government submits that a meaningful sentence is necessary and appropriate. The government therefore respectfully recommends a short term of imprisonment within the applicable U.S. Sentencing Guidelines range, which the Probation Office has calculated to be **0 to 6 months**, followed by a one-year term of supervised release.

BACKGROUND

On September 10, 2019, a criminal information was filed that charged the defendant with one count of misdemeanor computer fraud and abuse, in violation of 18 U.S.C. § 1030(a)(2)(C), (c)(2)(A), and (e)(1). The defendant appeared before this Court the same day. He pleaded guilty to the criminal information pursuant to a plea agreement. (*See* Plea Agreement, Dkt. 5.)

The defendant also has stipulated to have engaged in the conduct described in the Statement of Facts filed in this matter. (*See* Statement of Facts, Dkt. 6.) Specifically, the defendant admitted that sometime on or before October 30, 2018, he learned that his neighbor, J.B., had scheduled a press conference for purposes of releasing information that would allegedly discredit a particular government official and the investigation that official was conducting. The defendant already disliked J.B. from J.B.'s failure to fully compensate the defendant's wife for work she had performed for J.B., so the defendant decided he would retaliate against J.B. and protect the aforementioned official and investigation by gathering information from J.B.'s email account. (Presentence Investigation Report at ¶¶ 29, 37, 55, Dkt. 12.)

On October 30, 2018, the defendant put his plan into motion. Knowing his wife previously had acquired access to J.B.'s email account through her work for J.B., the defendant asked his wife to log into J.B.'s account in order to determine whether the credentials she had were still valid. The defendant's wife confirmed the credentials still worked, and the next day the defendant escalated his intrusion. On October 31, 2018, the defendant initially tried to log into J.B.'s account through the Tor network, which obfuscates Internet traffic, but was unsuccessful. The defendant and his wife then used their devices (without routing their traffic through Tor) to successfully log into J.B.'s account. The pair spent 15 to 20 minutes conducting searches within the account and reviewing, printing, photographing, and screenshotting emails of

interest. Although multiple popups appeared on the defendant's and his wife's devices questioning whether they had authorized access to the account, they remained in the account and even attempted to log back in after exiting the account. (*Id.* ¶¶ 19, 38–39.)

Although the defendant was employed by the FBI, the gathered information was not initially taken to law enforcement. Instead, the defendant and his wife tried to disseminate the information to the media and even offered to provide J.B.'s account password to a particular reporter. The reporter, however, did not accept the password, explaining it would be unethical to do so. (*Id.* ¶¶ 21, 40.)

On November 21, 2018, the defendant reported his conduct to the FBI, and provided the material he had taken from J.B.'s email account. The FBI subsequently investigated the defendant for his conduct. The defendant cooperated with the investigation, consenting to an interview and the search of his residence and devices. On November 27, 2018, the defendant's security clearance was suspended and he was removed from the FBI office at which he worked. Markedly, during this interaction, the defendant reiterated that he would do it all again because he believed his conduct was justified. (*Id.* ¶¶ 29-30, 41.)

SENTENCING ANALYSIS

I. Statutory Minimum and Maximum Penalties

The Defendant's conviction carries a maximum penalty of 1 year of imprisonment, a fine of $100,000, restitution and forfeiture, a special assessment, and 1 year of supervised release. (PSR at 1.)

II. Guidelines Range

A. Probation's Calculation

As reflected in paragraphs 57 through 65 of the PSR, the Probation Office has calculated the guidelines range for the Defendant's conviction as follows:

Guideline	Offense Level
Base Offense Level (Sections 2B1.1(a)(2))	6
Defendant was convicted of an offense under 18 U.S.C. § 1030, and the offense involved an intent to obtain personal information. (Section 2B1.1(b)(18))	+2
Acceptance of responsibility. (Section 3E1.1)	-2
TOTAL	**6**

Based on the defendant's Category I Criminal History, the resulting guidelines range would be 0 to 6 months of imprisonment. *Id.* at 17. The parties appear to be in agreement on the calculation of the Guidelines.

III. Sentencing Recommendation

As the Court is well aware, it must consult both the U.S. Sentencing Guidelines and the sentencing factors set forth in 18 U.S.C. § 3553(a) to determine the appropriate sentence for the defendant's crime of conspiracy to commit wire fraud. Although the Sentencing Guidelines are advisory, district courts are required to "consult those Guidelines and take them into account when sentencing." *United States v. Booker*, 543 U.S. 220, 264 (2005). As the Fourth Circuit has explained, district courts are to "first calculate (after making the appropriate findings of fact) the range prescribed by the guidelines. Then, the court shall consider that range as well as other

relevant factors set forth in the guidelines and those factors set forth in § 3553(a) before imposing the sentence." *United States v. Hughes*, 401 F.3d 540, 546 (4th Cir. 2005).[1]

Here, a short term of imprisonment followed by one year of supervised release is supported by several of the § 3553(a) factors, particularly the seriousness of the defendant's conduct, the need for deterrence, and the need to promote respect for the law.

We expect members of law enforcement to revere the law, not flout it. The defendant's disregard for the law is particularly troubling given the sequence of events. The defendant first tested his ability to access the account in question on one day, and then tried to access the account through the Tor network the next day presumably in an effort to hide his tracks. Once the defendant successfully accessed the account on October 31, he reviewed and exfiltrated a number of messages, and he even attempted to log into the account for a fourth time despite having received popup messages questioning his authority to access the account. This escalation of conduct shows that the defendant did not intrude into J.B.'s account on a whim; it was a premeditated, deliberate criminal act.

In this way, the defendant's conduct typifies the attitude of many toward cybercrime. There is a perception that computer intrusions carry high rewards and a relatively low risk of detection. The only way to affect this cost-benefit analysis is to impose meaningful sentences on those who are caught. *See United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006)

[1] The § 3553(a) factors include: the nature and circumstances of the offense and the history and characteristics of the defendant; the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, to provide just punishment for the offense, to afford adequate deterrence to criminal conduct, to protect the public from further crimes of the defendant, and to provide the defendant with needed training, medical care, or other treatment; the kinds of sentences available; the kinds of sentence and the sentencing range established for the type of offense committed; any pertinent policy statement; the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and the need to provide restitution to any victims of the offense.

(Because "economic and fraud-based crime are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence" (internal quotations and citation omitted)); *see also* U.S.S.G. Ch. 1, Pt. A(4)(d) (explaining that the Sentencing Commission crafted serious economic crimes Guidelines in order to remedy the pre-Guidelines sentencing "problem" of courts imposing probation on an "inappropriately high percentage" of white-collar offenders). If the Court imposes a meaningful sentence here, there is every reason to believe that many others who would consider engaging in computer intrusions will be deterred.

The defendant's attempt to minimize his conduct by virtue of his motivation for acting only serves to demonstrate why a meaningful sentence is necessary. For one, there is reason to question the purity of the defendant's motives. The defendant has expressed a distain for J.B. and indicated that a dispute over unpaid salary played a role in his conduct. Moreover, initially there was an attempt to pass the stolen information to the media. These admissions and conduct are at odds with the professed motive of acting to protect someone else. Moreover, these facts further underscore the need for a sentence that will promote respect for the law.

Yet, even if the defendant acted only to protect a federal official from false accusations, such conduct cannot be condoned. As the Fourth Circuit has recognized, "[n]o legal system could long survive if it gave every individual the option of disregarding with impunity any law which by his personal standard was judged morally untenable." *United States v. Moylan*, 417 F.2d 1002, 1009 (4th Cir. 1969). This is because "[t]oleration of such conduct would not be democratic . . . but inevitably anarchic." *Id.* Here, there simply is no justification for what the defendant did, and the defendant of all people should have understood this. His sentence therefore should demonstrate to the public the importance of adhering to the rule of law.

CONCLUSION

For the reasons stated above, the government submits that a short period of imprisonment followed by a 1-year term of supervised release is sufficient but not greater than necessary to satisfy the sentencing factors in § 3553.

Respectfully submitted,

G. Zachary Terwilliger
United States Attorney

Dated: December 13, 2019

By: /s/

Alexander P. Berrang
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Tel: (703) 299-3700
Fax: (703) 299-3981
Alexander.P.Berrang@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on December 13, 2019, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of filing (NEF) to counsel of record for the defense.

I also certify that on December 13, 2019, I will send a true and correct copy of the foregoing by e-mail to the following:

Leo R. Pet
United States Probation Officer
Leo_Pet@vaep.uscourts.gov

By: /s/
Alexander P. Berrang
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
Tel: (703) 299-3700
Fax: (703) 299-3981
Alexander.P.Berrang@usdoj.gov